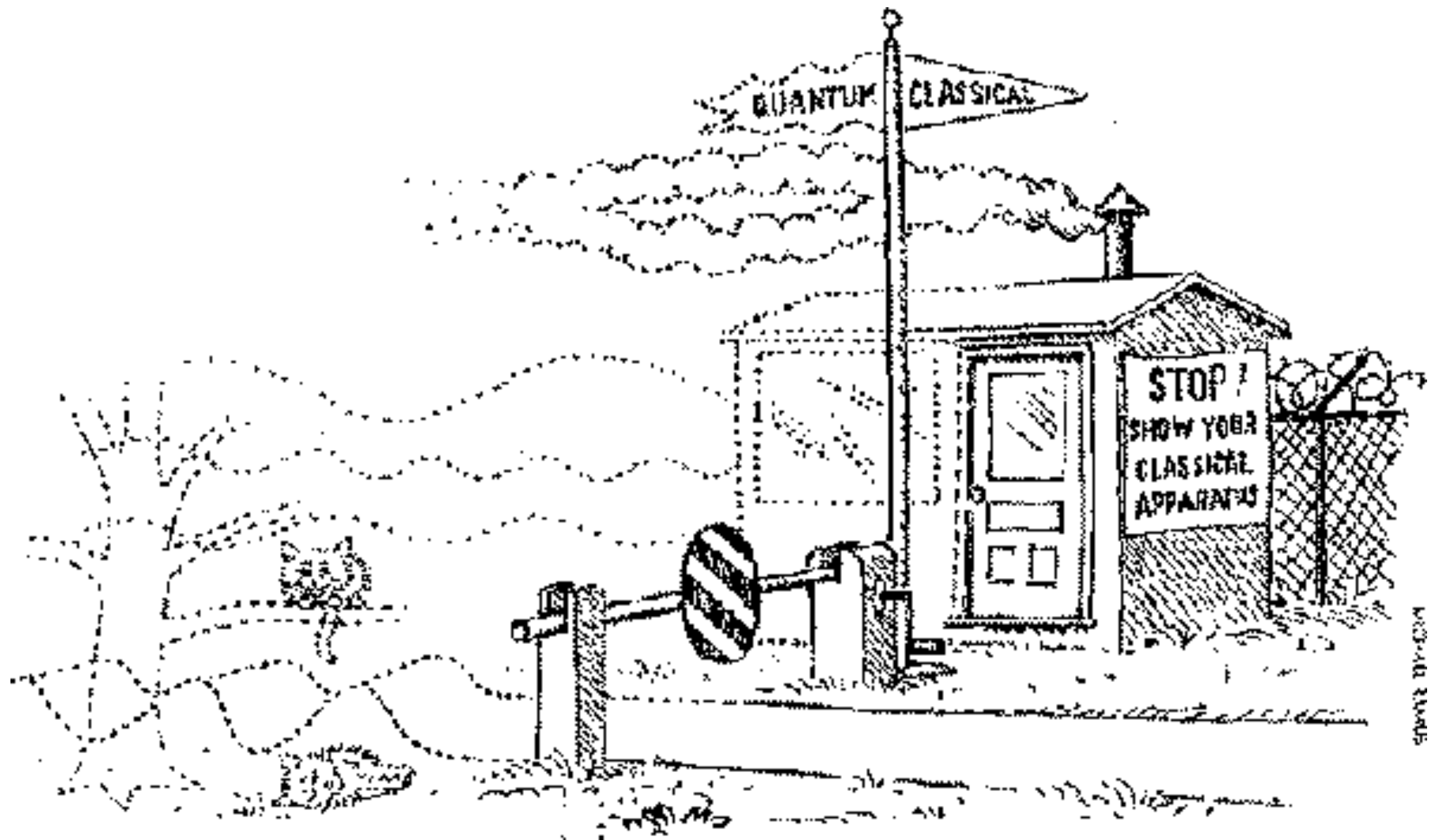


# Quantum Computing

---



# Information is Physical

---

information is always tied to a physical realization

## fundamental limits:

speed-limit:  $c$  (relativity)

resetting a bit costs  $> kT \ln 2$  (statistical mechanics)

dynamical RAM represents bit by charge on capacitor:

$b=1$  – capacitor charged

$b=0$  – capacitor uncharged

**Cbit**

alternative: **represent bit by spin- $\frac{1}{2}$**

$$|b\rangle = \alpha |0\rangle + \beta |1\rangle$$

superposition of (classical) bits

**Qbit**

Rolf Landauer



# Quantum Information

---

**Qbits cannot be copied**  
(no-cloning theorem)

**disadvantage:**  
information in Qbit not fully accessible  
(uncertainty!)

**advantage:**  
eavesdropping on a quantum channel detectable  
⇒ quantum cryptography

# No-Cloning Theorem

1. Kagi, J. H. R. & Nordberg, M. (eds) *Metallothionein* (Birkhauser, Basle, 1979).
2. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
3. Palido, P., Kagi, J. H. R. & Vallee, B. L. *Biochemistry* **5**, 1768–1777 (1966).
4. Rudol, C. J. & Herschmann, H. R. *Tox. appl. Pharmac.* **47**, 273–278 (1979).
5. Karin, M. & Herschman, H. R. *Eur. J. Biochem.* **107**, 395–401 (1980).
6. Kissling, M. M. and Kagi, J. H. R. *FEBS Lett.* **82**, 247–250 (1977).
7. Karin, M. *et al. Nature* **286**, 295–297 (1980).
8. Karin, M., Slater, E. P. & Herschman, H. R. *J. cell. Physiol.* **106**, 63–74 (1981).
9. Durnam, D. M. & Palmiter, R. D. *J. biol. Chem.* **256**, 5712–5716 (1981).
10. Hager, L. J. & Palmiter, R. D. *Nature* **291**, 340–342 (1981).
11. Karin, M. & Richards, R. *Nucleic Acids Res.* **10**, 3165–3173 (1982).
12. Lawn, R. M. *et al. Cell* **15**, 1157–1174 (1978).
13. Southern, E. M. *J. molec. Biol.* **98**, 503–517 (1975).
14. Benton, W. D. & Davis, R. W. *Science* **196**, 180–182 (1977).
15. Gianville, N., Durnam, D. M. & Palmiter, R. D. *Nature* **292**, 267–269 (1981).
16. Breathnach, R. *et al. Proc. natn. Acad. Sci. U.S.A.* **75**, 4853–4857 (1978).
17. Weaver, R. F. & Weissman, C. *Nucleic Acids Res.* **5**, 1175–1193 (1979).
18. Kayb, K. E., Warren, R. & Palmiter, R. D. *Cell* **29**, 99–108 (1982).
19. Brinster, R. L. *et al. Nature* **296**, 39–42 (1982).

20. Kingsbury, R. & McKnight, S. L. *Science* **217**, 316–324 (1982).
21. Larsen, A. & Weintraub, H. *Crit* **29**, 609–672 (1982).
22. Proudfoot, N. J. & Brownlee, G. G. *Nature* **263**, 211–214 (1976).
23. Proudfoot, N. J. & Miller, J. H. *Cell* **20**, 579–595 (1978).
24. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
25. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
26. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
27. Jagadeeswaran, P., Forget, B. G. & Weissman, S. M. *Cell* **26**, 141–142 (1982).
28. Nishioka, Y., Leder, A. & Leder, P. *Proc. natn. Acad. Sci. U.S.A.* **77**, 2806–2809 (1980).
29. Wilde, C. D. *et al. Nature* **297**, 83–84 (1982).
30. Shaul, Y., Kaminichik, I. & Aviv, H. *Eur. J. Biochem.* **116**, 461–466 (1981).
31. Perry, R. P. *et al. Proc. natn. Acad. Sci. U.S.A.* **77**, 1937–1941 (1980).
32. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
33. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
34. Karin, M. & Herschman, H. R. *Science* **204**, 176–177 (1979).
35. Wahl, R. M., Stern, M. & Stark, G. R. *Proc. natn. Acad. Sci. U.S.A.* **76**, 3683–3687 (1979).
36. Maxam, A. & Gilbert, W. *Meth. Enzym.* **65**, 499–559 (1980).
37. Sanger, F., Nicklen, S. & Coulson, A. R. *Proc. natn. Acad. Sci. U.S.A.* **74**, 5463–5468 (1979).
38. Goodman, H. M. *Meth. Enzym.* **65**, 63–64 (1980).
39. Heidecker, G., Messing, R. O. & Messing, R. O. *Proc. natn. Acad. Sci. U.S.A.* **77**, 1937–1941 (1980).
40. O'Farrell, P. *Focus* **3**, 1–10 (1982).

Wootters&Zurek Nature 299, 802 (1982)  
it is impossible to copy an unknown quantum state  
proof by reductio ad absurdum

## LETTERS TO NATURE

### A single quantum cannot be cloned

W. K. Wootters\*

Center for Theoretical Physics, The University of Texas at Austin,  
Austin, Texas 78712, USA

W. H. Zurek

Theoretical Astrophysics 130–33, California Institute of Technology,  
Pasadena, California 91125, USA

If a photon of definite polarization encounters an excited atom, there is typically some nonvanishing probability that the atom will emit a second photon by stimulated emission. Such a photon is guaranteed to have the same polarization as the original photon. But is it possible by this or any other process to amplify a quantum state, that is, to produce several copies of a quantum system (the polarized photon in the present case) each having the same state as the original? If it were, the amplifying process could be used to ascertain the exact state of a quantum system: in the case of a photon, one could determine its polarization by first producing a beam of identically polarized copies and then measuring the Stokes parameters<sup>1</sup>. We show here that linearity of quantum mechanics forbids such replication and that this conclusion holds for all quantum systems.

Note that if photons could be cloned, a plausible argument could be made for the possibility of faster-than-light communication<sup>2</sup>. It is well known that for certain non-separably correlated Einstein–Podolsky–Rosen pairs of photons, once an observer has made a polarization measurement (say, vertical versus horizontal) on one member of the pair, the other one, which may be far away, can be for all purposes of prediction regarded as having the same polarization<sup>3</sup>. If this second photon could be replicated and its precise polarization measured as above, it would be possible to ascertain whether, for example, the first photon had been subjected to a measurement of linear or circular polarization. In this way the first observer would be able to transmit information faster than light by encoding his message into his choice of measurement. The actual impossibility of cloning photons, shown below, thus prohibits superluminal communication by this scheme. That such a scheme must fail for some reason despite the well-established existence of long-range quantum correlations<sup>6–8</sup>, is a general consequence of quantum mechanics<sup>9</sup>.

A perfect amplifying device would have the following effect

on an incoming photon with polarization state  $|s\rangle$ :

let  $U$  be unitary cloning operator:  $U|\psi\rangle|s\rangle = |\psi\rangle|\psi\rangle$  for any  $|\psi\rangle$   
then  $\langle s|\langle\psi|U^\dagger \cdot U|\phi\rangle|s\rangle = \langle s|s\rangle\langle\psi|\phi\rangle$   
 $|A_0\rangle|\uparrow\rangle \rightarrow |A_{\text{ver}}\rangle|\uparrow\uparrow\rangle$  (2)

and

$|A_0\rangle|\leftrightarrow\rangle \rightarrow |A_{\text{hor}}\rangle|\leftrightarrow\leftrightarrow\rangle$  (3)  
def  $\langle\psi|\langle\psi| \cdot |\phi\rangle|\phi\rangle = \langle\psi|\phi\rangle^2$

According to quantum mechanics this transformation should be reproducible by a linear cloning operator. It therefore follows that if the cloning process were linear, the polarization given by the linear combination  $\alpha|\uparrow\rangle + \beta|\leftrightarrow\rangle$ —for example, it could be linearly polarized in a direction 45° from the vertical, so that  $\alpha = \beta = 2^{-1/2}$ —the result of its interaction with the apparatus will be the superposition of equations (2) and (3):

$|A_0\rangle(\alpha|\uparrow\rangle + \beta|\leftrightarrow\rangle) \rightarrow \alpha|A_{\text{ver}}\rangle|\uparrow\uparrow\rangle + \beta|A_{\text{hor}}\rangle|\leftrightarrow\leftrightarrow\rangle$  (4)  
If the apparatus were linear,  $|A_{\text{ver}}\rangle$  and  $|A_{\text{hor}}\rangle$  would be identical, then the two photons emerging from the apparatus would be in a mixed state of polarization. If these apparatus states are identical, then the two photons are in the pure state

$$\alpha|\uparrow\uparrow\rangle + \beta|\leftrightarrow\leftrightarrow\rangle \quad (5)$$

In neither of these cases is the final state the same as the state with two photons both having the polarization  $\alpha|\uparrow\rangle + \beta|\leftrightarrow\rangle$ . That state, the one which would be required if the apparatus were to be a perfect amplifier, can be written as

$$2^{-1/2}(\alpha a_{\text{ver}}^+ + \beta a_{\text{hor}}^+)^2|0\rangle = \alpha^2|\uparrow\uparrow\rangle + 2^{1/2}\alpha\beta|\uparrow\leftrightarrow\rangle + \beta^2|\leftrightarrow\leftrightarrow\rangle$$

which is not a pure state. Thus no apparatus exists which will amplify an arbitrary polarization. The above argument does not rule out the possibility of a device which can amplify two special polarizations, such as vertical and horizontal. Indeed, any measuring device which distinguishes between two special polarizations, such as vertical and horizontal, could be used to amplify them.

The same argument can be applied to any other kind of quantum system. As in the case of photons, linearity does not forbid the amplification of any given state by a device designed especially for that state, but it does rule out the existence of a device capable of amplifying an arbitrary state.

Milonni (unpublished work) has shown that the process of stimulated emission does not lead to quantum amplification, because if there is stimulated emission there must also be with equal probability the emission of a photon in the opposite direction. The emission of a photon in the opposite direction of a stimulated photon is entirely independent of the polarization of the original.

It is conceivable that a more sophisticated amplifying apparatus could get around Milonni's argument. We have therefore considered the possibility of a device which has in the input a photon in a known polarization state, and which produces, however complicated, can amplify an arbitrary polarization.

We stress that the question of replicating individual photons is of practical interest. It is obviously closely related to the

1. Born, M. & Wolf, E. *Principles of Optics* 4th edn (Pergamon, New York, 1970).
2. Herbert, N. *Found. Phys.* (in the press).
3. Einstein, A., Podolsky, B. & Rosen, N. *Phys. Rev.* **47**, 777–780 (1935).
4. Bohm, D. *Quantum Theory*, 611–623 (Prentice-Hall, Englewood Cliffs, 1951).
5. Kocher, C. A. & Commins, E. D. *Phys. Rev. Lett.* **18**, 575–578 (1967).
6. Freedman, S. J. & Clauser, J. R. *Phys. Rev. Lett.* **28**, 938–941 (1972).

The Crab Nebula's progenitor  
Ken'ichi Nomoto\*, Warren M. Sparks†,  
Robert A. Fesen‡, Theodore R. Gull‡, S. Miyaji‡  
unitary

\* Department of Earth Science, Williams College, Williamstown,  
Tokyo, College of General Education, 1-8-1, Kamata, Meguro,  
Tokyo 153, Japan  
† Group X-5, Mail Stop F665, Los Alamos National Laboratory,  
Los Alamos, New Mexico 87545, USA  
‡ Laboratory for Astronomy and Solar Physics, Goddard Space  
Flight Center, Greenbelt, Maryland 20771, USA

The study of supernovae is hampered by our limited knowledge of initial stellar mass for individual stars. Because of large uncertainties in estimating both the total mass of a remnant (including the pulsar or black hole) and any mass loss during the pre-supernova stages, the main sequence mass of the progenitor cannot be accurately determined from observations alone. To calculate an initial mass, one must rely on a combination of both theory and observation. Limits on the progenitor mass range can be obtained by the presence of a remnant and its composition. The observed neon chemical abundances with detailed evolutionary calculations<sup>1</sup>. The Crab Nebula is an excellent choice for investigation because it contains a unique combination of characteristics: a central neutron star (pulsar) and a bright, well studied nebula having little or no swept-up interstellar material. In fact, several studies<sup>1–4</sup> have suggested an initial mass of  $\sim 10 M_\odot$  for the Crab progenitor. Recently, Davidson *et al.*<sup>5</sup>, quoting two of us (K.N. and W.M.S.), state that the Crab's progenitor had a mass slightly larger than  $8 M_\odot$ . Here we present in detail the reasoning behind this statement and suggest the explosion mechanism.

Briefly, the Crab consists of a pulsar (assumed here to have a mass of  $1.4 M_\odot$ ) and a nebula (assumed to have a mass of  $1.7 \times 10^4 M_\odot$ ) (where  $X$  is an element's mass fraction). The oxygen abundance ( $X_O$ ) is  $\sim 0.003$  (refs 5, 6), which is less than the solar value of 0.007, while the oxygen-to-hydrogen ratio is approximately solar. The carbon-to-oxygen ratio is  $0.4 < X_C/X_O < 1.1$  (ref. 5). The progenitor was oxygen-rich, while neon, sulphur and iron abundances are probably not greatly over- or underabundant. Because the Crab Nebula is helium-rich but not oxygen-rich, the hydrogen-rich (solar abundances) envelope and the helium layer of the progenitor star were ejected but the oxygen-rich layer below the helium layer was not. The lower layers must have formed the neutron star. The

quantum limits on the noise in amplifiers<sup>10,11</sup>. Moreover, an experiment devised to establish the extent to which polarization of single photons can be replicated through the process of stimulated emission is under way (A. Gozzini, personal communication; and see ref. 12). The quantum mechanical prediction is quite definite; for each perfect clone there is also one randomly polarized, spontaneously emitted, photon.

We thank Alain Aspect, Carl Caves, Ron Dickman, Ted Jacobsen, Peter Milonni, Marlan Scully, Pierre Meystre, Don Page, and an Archibald Wheeler for enjoyable and stimulating

This work was supported in part by the NSF (PHY 78-26592 and AST 79-22012-A1). W.H.Z. acknowledges a Richard Chace Tolman Fellowship.

7. Fry, E. S. & Thompson, R. C. *Phys. Rev. Lett.* **37**, 465–468 (1976).
8. Aspect, A., Grangier, P. & Roger, G. *Phys. Rev. Lett.* **47**, 460–463 (1981).
9. Bussey, P. J. *Phys. Lett.* **90A**, 9–12 (1982).
10. Haus, H. A. & Mullen, J. A. *Phys. Rev.* **128**, 2407–2410 (1962).
11. Caves, C. M. *Phys. Rev. D15*, (in the press).
12. Gozzini, A. *Proc. Symp. on Wave-Particle Duality* (eds Diner, S., Fargue, D., Lochak, G. & Selleri, F.) (Reidel, Dordrecht, in the press).

low, the helium-to-hydrogen ratio means that at the time of the explosion the material must have come from the helium layer.

Arnett (ref. 7 and refs therein) systematically evolved helium cores of various masses ( $M_\odot$ ) into late stages of evolution. He<sup>1</sup> compared Davidson's<sup>8</sup> derived abundances of the Crab nebula with calculated abundances from the  $M_\odot = 4.0 M_\odot$  model, which was his lowest-massed, highly evolved helium core (corresponding to approximately a  $15 M_\odot$  star). Combining all the material above the helium-burning shell (his case B) with enough interstellar material to obtain  $X_{\text{He}}/X_{\text{H}} = 8$ , he found good agreement with  $X_{\text{N}}/X_{\text{He}}$  and  $X_{\text{O}}/X_{\text{He}}$  of Davidson's<sup>8</sup> 'model 1'. However, the calculated value of  $X_{\text{C}}/X_{\text{He}}$  was too large by a factor of 30. At that time, the Crab's carbon abundance had not been directly measured and Arnett suggested several possibilities: the inferred carbon abundance was too low, the carbon was hidden in the filaments, or a lower-mass helium core,  $\sim 3 M_\odot$ , was more appropriate.

Using recent UV observations with the International Ultraviolet Explorer, Davidson *et al.*<sup>5</sup> have established that the carbon abundance is nearly solar. They also showed that the hydrogen and helium seemed to be fairly well mixed and, as carbon is convectively mixed in the helium layer, this would argue against carbon being hidden in the filaments. However, the observations by Dennefeld and Andriolat<sup>9</sup> showed that the strength of [C I]  $\lambda 9,850$  relative to [S III]  $\lambda 9,069$  varied with position in the Crab. The strongest [C I] line would indicate a rather large carbon abundance if the ionizing flux is constant. Whether the IR observations indicate variation in the carbon abundance, variation in the ionizing flux, or high densities in neutral cores is not known. For the remainder of this report we will assume the carbon abundance as determined by Davidson *et al.*<sup>5</sup>.

The existence of a pulsar in the Crab indicates that the progenitor's mass was larger than the upper mass limit ( $8 \pm 1 M_\odot$ )<sup>10</sup> for degenerate carbon ignition. Degenerate carbon ignition results in carbon deflagration<sup>11</sup> which completely disrupts the star, leaving no compact remnant. Lower-mass stars that lose enough mass to avoid degenerate carbon burning eventually become white dwarfs. Stars massive enough ( $\geq 8 M_\odot$ ) to burn carbon non-degenerately will eventually undergo a core collapse initiated either by electron capture<sup>12</sup> onto Mg, Ne and O or by burn-out of all the available fuel<sup>13,14</sup>. When the collapsing core reaches neutron-star densities, stability is regained. Although detailed calculations of the collapse remain inconclusive, it is generally felt that the core will overshoot its equilibrium position and then rebound, initiating a shock wave<sup>4</sup>. This shock wave ejects the outer material but not the core, resulting in both a supernova nebula and a pulsar<sup>15</sup>. In more massive stars

\* Present address: Department of Physics and Astronomy, Williams College, Williamstown, Massachusetts 01267, USA.

# quantum parallelism

---

$$U_H|0\rangle U_H|0\rangle \dots U_H|0\rangle = U_H^{\otimes n}|00\dots 0\rangle = \sum_{\mathbf{x}} |\mathbf{x}\rangle$$

superposition of all  $2^n$  basis states

implement classical function  $f(x)$  as unitary operator:

$$U_f|\mathbf{x}\rangle|\mathbf{y}\rangle := |\mathbf{x}\rangle|\mathbf{y} \oplus f(\mathbf{x})\rangle$$

then 
$$U_f U_H^{\otimes n}|\mathbf{0}\rangle|\mathbf{0}\rangle = U_f \sum_{\mathbf{x}} |\mathbf{x}\rangle|\mathbf{0}\rangle = \sum_{\mathbf{x}} \underbrace{|\mathbf{x}\rangle|f(\mathbf{x})\rangle}_{\mathbf{x} \text{ and } f(\mathbf{x}) \text{ entangled!}}$$

simultaneous evaluation of  $2^n$  function values

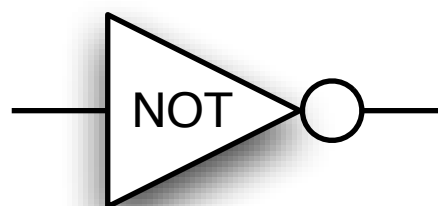
**problem:** only one (random!)  $f(x)$  can be measured

# classical logics

## Boolean operations

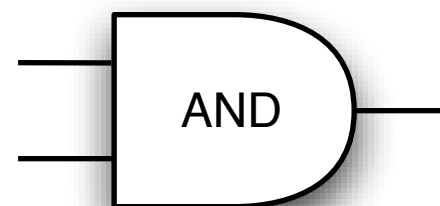
NOT gate

a	$\neg a$
0	1
1	0



AND gate

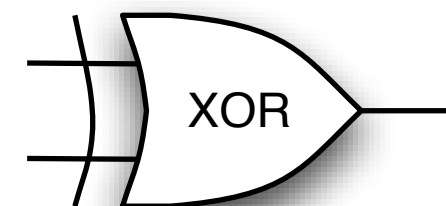
a	b	$a \cdot b$
0	0	0
0	1	0
1	0	0
1	1	1



not reversible!

XOR gate

a	b	$a \oplus b$	a
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1



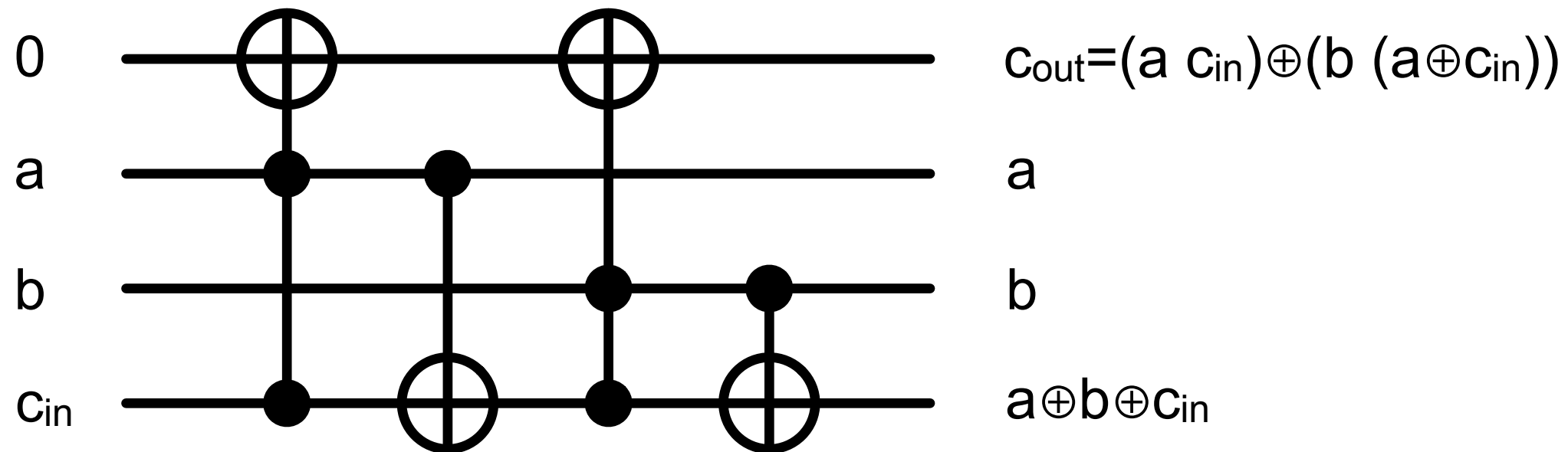
reversible: cNOT



# reversible logics

e.g. controlled NOT and Toffoli gates

example:  
full adder



reversible gate defines operation on basis states  
naturally extends to unitary operators

quantum gates without classical analogon:  
e.g. Hadamard gate (creates superpositions)

$$U_H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$U_H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

# Quantum Computing

---

notion of computability unchanged  
quantum systems can be simulated on a classical computer

computational complexity reduced:  
quantum computers can be much faster than classical ones

problem	classical algorithm	quantum algorithm
factoring $N$	number field sieve $O(e^{\sqrt[3]{N}})$	Shor algorithm:
unstructured search in $N$ items	brute force: $O(N)$	Grover algorithm: $O(\sqrt{N})$

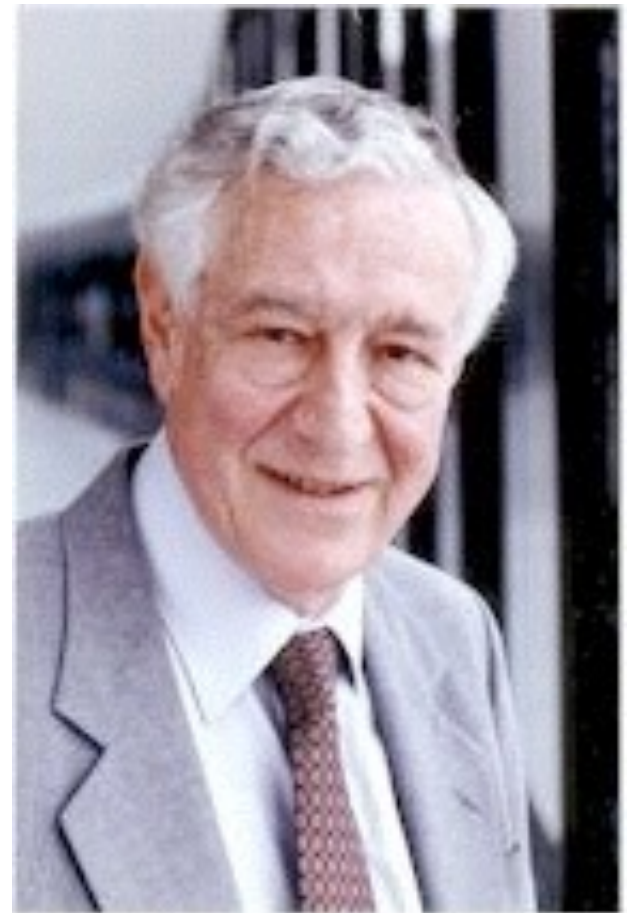


# Landauer's Disclaimer

---

Nature **400**, 720 (1999)

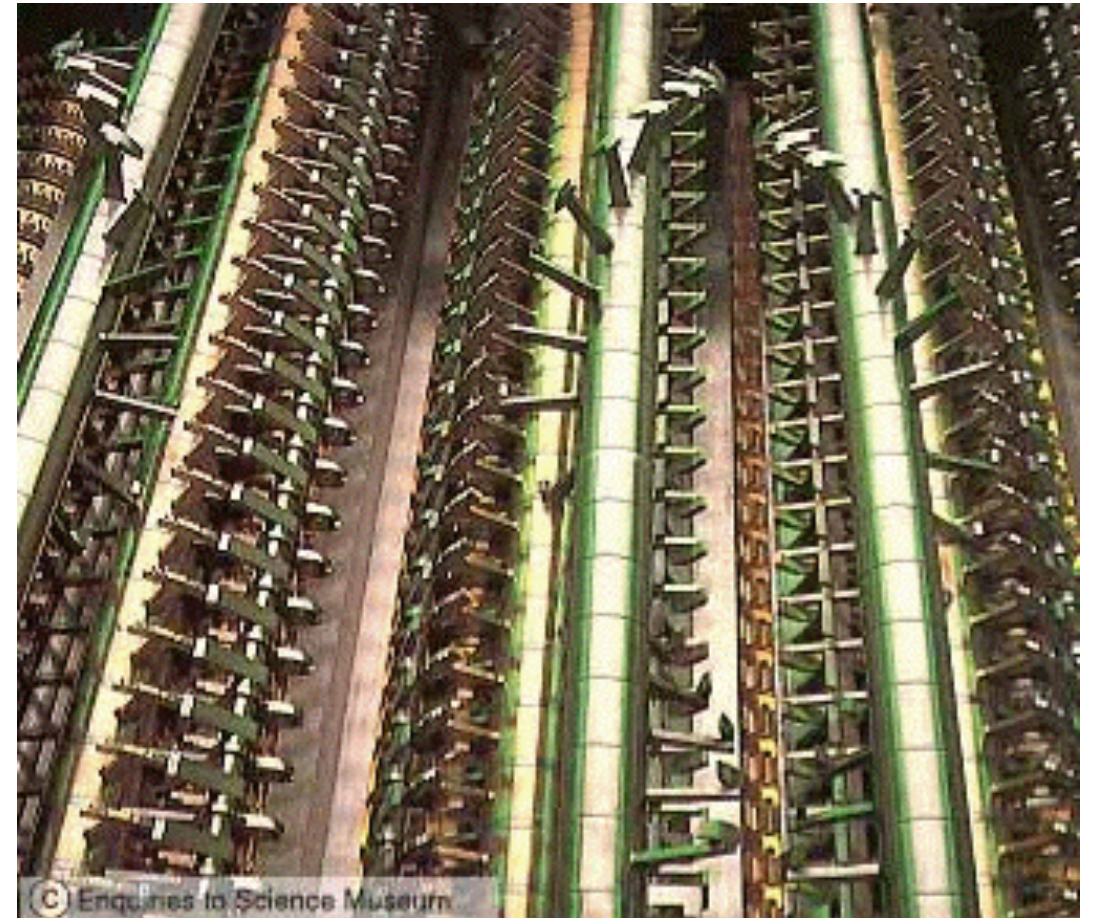
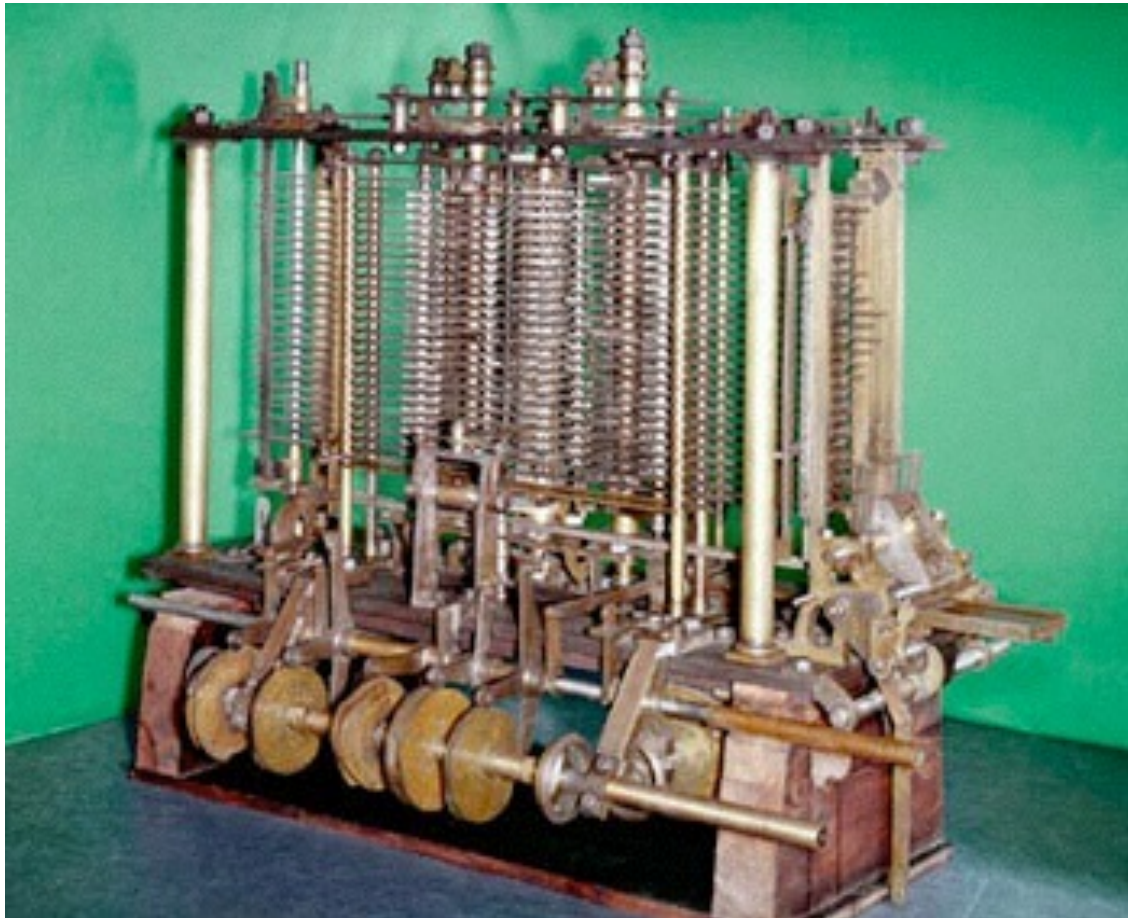
This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manufacturing error, and probably will not work.



# inappropriate hardware

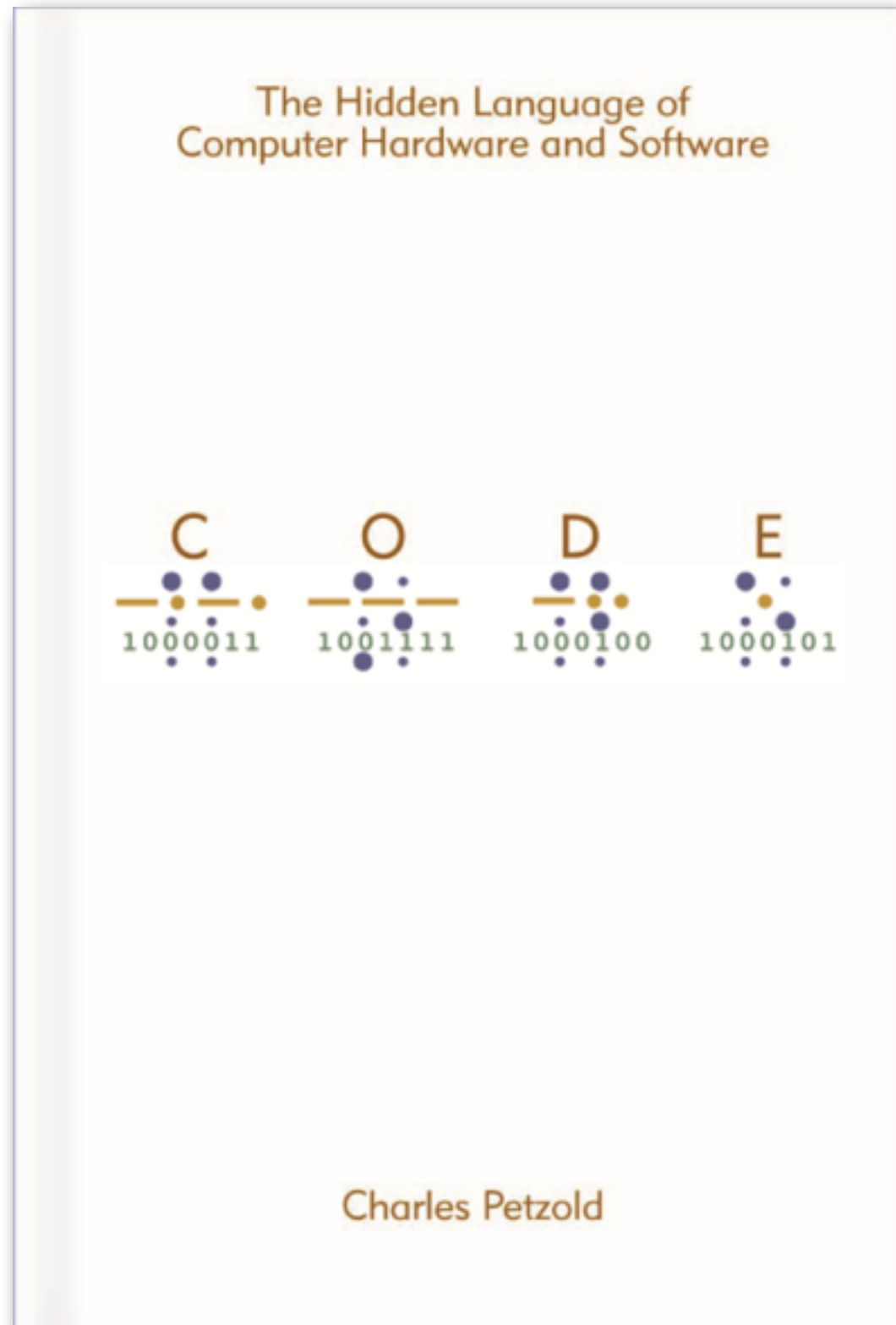
---

mechanical computers

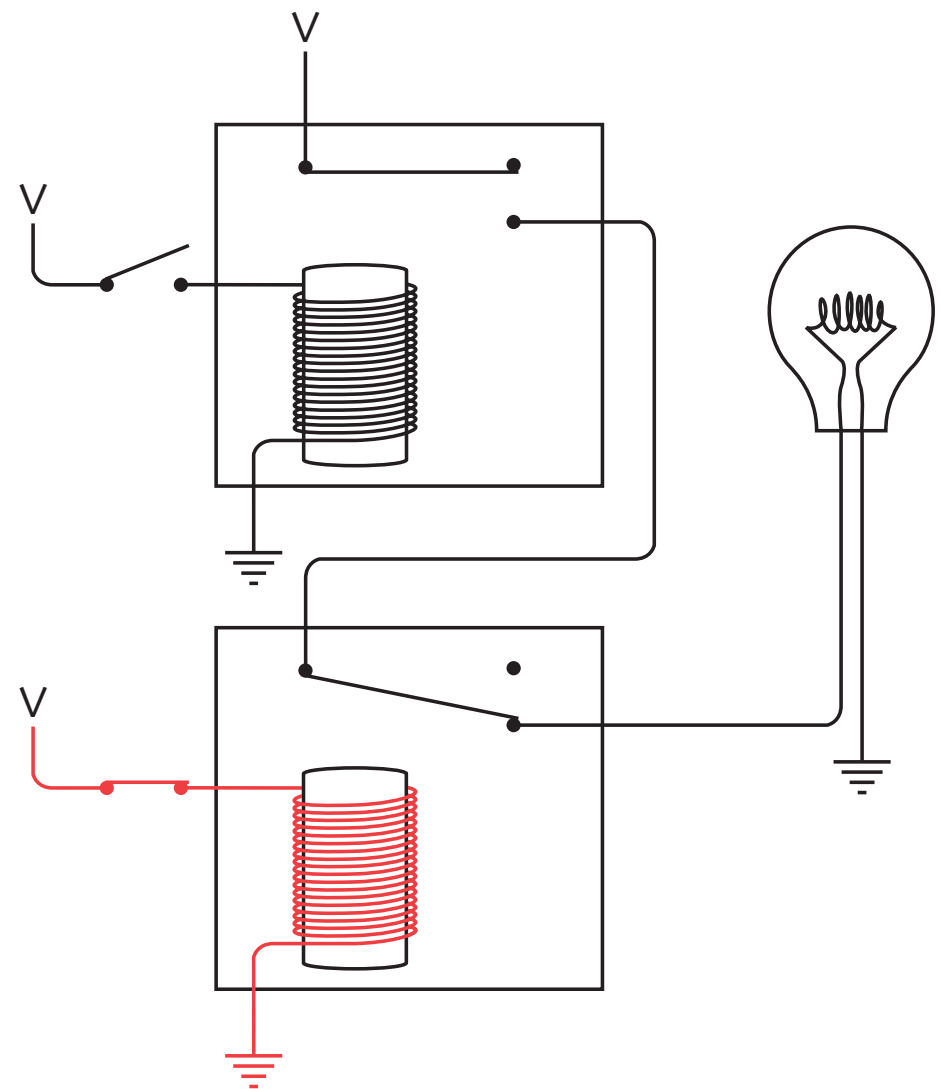


Charles Babbage: Analytical Engine (1834)

# how to build a computer from relays



Charles Petzold: **Code**  
The Hidden Language of  
Computer Hardware and Software  
Microsoft Press, 2000





# Quantum Cryptography



MagiQ: [www.magiqtech.com](http://www.magiqtech.com)  
id quantique: [www.idquantique.com](http://www.idquantique.com)



Figure 3: id Quantique's system exchanged keys over 67 km of standard optical fiber.

# Confused?

---

Möglicherweise ist es, nebenbei gesagt, für die Kopenhagener Interpretation der Quantenmechanik wichtig, dass ihre Sprache in einem gewissen Grad unbestimmt ist, und ich bezweifle, dass sie durch den Versuch, diese Unbestimmtheit zu vermeiden, klarer werden kann. (W. Heisenberg)

